They're Building a National Digital ID And Calling It Child Safety

CONSERVATIVE LADIES OF AMERICA
MAR 19, 2026

If you've been following our reporting on AI legislation, you already know the playbook: take a surveillance architecture nobody would vote for on its own, wrap it in child safety language, and dare anyone to vote against it. That playbook has taken on a new, larger form at the federal level.

It's called the RUMP AI Act (yes, really...*Republic Unifying Meritocratic Performance Advancing Machine intelligence by Eliminating Regulatory Interstate Chaos Across American Industry Act*), and it was introduced by Sen. Marsha Blackburn (R-TN). On the surface, the bill's goals sound like

everything Americans have been asking for: protect children from harmful AI, stop Big Tech censorship, defend creators, and promote American innovation.

But here's the first thing you need to understand about this bill: it is not one bill. It is **seventeen bills crammed into 291 pages** and presented as a single piece of legislation. It bundles child safety provisions, Section 230 repeal, copyright law, agency AI governance, anti-bias audits, content watermarking, and a national AI research infrastructure, all under one roof, all in one vote.

That structure is not an accident. We recently saw this on the House side, wrapping 7 tech "protect the children" policies wrapped into one. It's an effective strategy...not necessarily "good", but effective. When you package seventeen different policy areas into one bill, the provisions that would never survive on their own get carried across the finish line by the ones that would. And the ones most people will never read, the ones buried in the technical language of Titles V and VI, are the ones that matter most.

Underneath the child safety framing, this bill builds the architecture for a **national Digital ID system**. And the mechanism it uses to get there is one that will be very difficult to argue against: protecting your kids.

Let's walk through exactly how it works.

The Age Verification Tripwire

The child protection provisions are where most people will stop reading. Of course we want to protect children. Nobody is arguing against that. But the mechanism this bill uses to achieve that goal should give every parent pause.

Title V — the GUARD Act — requires the following:

- Every user of an AI chatbot must create an account before accessing it
- Every account must be age-verified using a *"reasonable age verification measure"*
- The bill defines that measure explicitly as: **a government-issued identification**, or an equivalent commercial method

Under this bill, you would be required to present government-issued ID to access an AI chatbot.

And it doesn't stop there.

Section 417 mandates a federal study on implementing age verification at the **device or operating system level**, meaning your phone or computer itself would be required to verify your identity before allowing access to certain content. The government is openly studying how to bake a digital identity layer into consumer hardware.

These two provisions together; ID at the account level today, ID at the device level tomorrow, are not separate ideas. They are **sequential steps in the same infrastructure project**.

We've seen this pattern over and over during the last year where the language of child protection is used to justify identity verification requirements that go far beyond what child safety actually requires. The architecture is always the same.

We read the bills so you don't have to. But that work isn't free. No corporate donors, no lobbyist money, just readers like you. Consider upgrading to a paid subscription to keep this work going

✔ Subscribed

Duty of Care Means Surveillance…Full Stop

Here is something the bill's supporters will not tell you: **you cannot have duty of care without monitoring.**

Title I of the bill imposes a legal duty of care on AI developers, requiring them to prevent "reasonably foreseeable harms" to users. That sounds protective but think through what it actually requires in practice.

If a platform is legally liable for harms to users, they must be able to demonstrate in court that they were watching for those harms, flagging them, and intervening. Duty of care is not a passive standard, it is an active surveillance obligation dressed up in the language of responsibility.

The chain reaction looks like this:

1. The bill imposes duty of care on platforms
2. Platforms must monitor user interactions to demonstrate compliance
3. Monitoring requires persistent, identity-linked accounts, which the bill also requires
4. Identity-linked accounts require age verification, which the bill also requires
5. Age verification requires government ID, which the bill also requires

These are not separate provisions they are **a single integrated system**, each piece making the next piece legally and operationally necessary. The duty of care provision is not a standalone child protection measure, rather it is the justification that makes all the surveillance infrastructure that follows legally defensible.

Who Gets Your Identity Data?

Section 503 allows covered entities to contract with **third-party age verification providers** to carry out identity verification. These are often data brokers; companies whose entire business model is the collection, aggregation, and monetization of personal data. *(Fun fact: these age verification providers are testifying in support of these policies around the country as they stand to make a lot of money if these laws are enacted!)*

The bill includes some data minimization language. But it contains **no prohibition on those third parties retaining your verified identity data** for other purposes. No restriction on selling it. No hard limit on how long they can keep it.

Here is what the pipeline looks like in practice:

1. You want to use an AI chatbot
2. You are required to create an account
3. That account requires age verification
4. The company outsources verification to a third-party data broker
5. The data broker now has your government-verified identity linked to your AI usage
6. Nothing in this bill prevents them from selling that data

That is not a hypothetical, that is the very pipeline this bill creates and leaves unguarded.

The Government Gets a Copy Too

Title VI, Section 602 requires every covered AI developer to hand over to the Department of Energy, on request the following:

- The underlying source code of their AI system
- All data used to train the system

- Model weights and adjustable parameters
- The interface engine and implementation details
- Detailed information about training methodology and architecture

Non-compliance bars the company from deploying their AI in interstate commerce. The fine for violations is **$1,000,000 per day**.

The federal government can demand the complete technical blueprint of any major AI system without a warrant, without individualized suspicion, as a routine condition of operating. Constitutional attorneys will note that source code has been recognized as protected speech, and compelling its handover without a warrant raises serious First, Fourth, and Fifth Amendment concerns. But the constitutional problems don't make the political problem disappear: this is the government inserting itself into the internals of every major AI platform in America.

The FTC Gets the Keys to the Kingdom

Throughout this bill, in Title I, Title IV, Title V, and Title VIII, Congress hands the Federal Trade Commission sweeping authority to "promulgate rules establishing minimum reasonable safeguards."

That means Congress is not actually writing the rules. Instead, they are writing a permission slip and handing it to an unelected federal agency.

The FTC will decide:

- What counts as "harm" from an AI chatbot
- What "reasonable safeguards" look like
- What platforms must do to comply
- How to enforce violations

Here is the problem with that (and it is a problem regardless of which party is currently in power): these rules will outlast any administration.

The framework being built today will be operated by whoever controls the FTC tomorrow. A future commission could define “harmful” AI content to include anything that conflicts with the ideological priorities of the moment, and the enforcement machinery this bill creates will already be in place, ready to use.

This is not a theoretical concern; it is how federal regulatory power has worked every single time it has been expanded.

What About the “Wins”?

You may have seen this bill promoted in conservative circles as a package of wins: Section 230 repeal, anti-DEI language, anti-censorship provisions. It is worth looking at each of those claims carefully.

Section 230 repeal is something conservatives have demanded for years as a way to hold Big Tech accountable for censorship. But full repeal removes *both* of Section 230’s protections, including the one that shields platforms from liability for content posted by users. Without that shield, every platform hosting user-generated content becomes a litigation target. The platforms with the legal teams and resources to absorb that exposure are the large ones. The platforms that cannot are the small Christian and conservative alternatives that your community has been building. Full repeal may silence the little guys while Big Tech’s legal armies manage just fine.

The anti-bias and anti-DEI language in Title VIII and Title XVI sounds like a meaningful commitment to ideological neutrality in AI. But bias audits are only as neutral as the people conducting them. Anti-DEI procurement rules are only as meaningful as the administration enforcing them. The same legal framework that bans DEI-coded AI procurement today gives a future Democrat administration a fully-built regulatory apparatus to define bias however they choose.

The content provenance and watermarking provisions in Title XIV require machine-readable metadata to be attached to all AI-generated content in a way that cannot be easily removed. The stated purpose is preventing deepfakes, however, the structural reality is a **traceable chain of origin for all AI-generated speech**, including AI-assisted political commentary, religious content, and journalism. In the hands of a future government hostile to those viewpoints, that infrastructure becomes a targeting system.

This Is the National Template

The federal government has made clear it wants one unified AI framework rather than fifty different state laws. That is why the Trump administration has been pushing back on state-level bills. A centralized system is easier to control, enforce, and integrate into existing federal agencies than a patchwork of state rules.

But the bill being pushed at the federal level by a Republican senator builds **the exact same identity-linked, always-on monitoring architecture** that states have been criticized for pursuing. The framing is different. The political branding is different. The acronym is different. But the structure of mandatory accounts, government ID verification, third-party data brokers, federal agency access, behavioral monitoring obligations is exactly the same.

Seventeen policy areas. One vote. And buried in the middle of it, a Digital ID infrastructure that no one would vote for if it were introduced on its own.

What You Can Do

This bill is still in the early stages introduced this week by Sen. Blackburn and referred to committee. That means there is still time to

demand changes.

The provisions that must be addressed before this bill moves forward:

- The government-ID age verification requirement in Title V must be removed or replaced with a privacy-preserving alternative that does not create a national digital identity checkpoint
- The device/OS-level age verification study in Section 417 must be stripped from the bill entirely
- The source code handover requirement in Section 602 must require a warrant and individualized legal process
- The FTC rulemaking delegations must be specific and bounded, not open-ended permission slips
- Data broker involvement in age verification must be explicitly prohibited or strictly regulated

Contact your senators. Tell them you support protecting children from AI harms and that you oppose any provision that requires government ID to access the internet, that hands your identity to data brokers, or that gives unelected federal agencies unchecked authority over digital speech.

You can find your senators at https://www.senate.gov/senators/senators-contact.htm

And as always, share this article. The bills that become law are the ones most people never read. Help us change that.

Share

Support Our Work

If you've been following our journey, you know we don't sit on the sidelines. We show up in committee rooms, we read the bills no one else is reading, and we speak truth into spaces dominated by lobbyists and political insiders. But we can only do this because everyday Americans choose to stand with us.

Conservative Ladies has no corporate backers or deep-pocket donors, just citizens and families who care about protecting children and preserving our freedoms. If this work matters to you, we would be grateful for your partnership. Whether it's a monthly subscription or a one-time gift of any amount, your support fuels our ability to educate, equip, and be a voice for "We the People" across the country. Thank you for standing with us as we continue this fight.

DONATE

Subscribed